4 Design

4.1 Design Context

4.1.1 Broader Context

The communities this project is being designed for encapsulates many communities across the globe. However, most importantly, this will directly impact the daily commuters, public transportation, and any commonly used heavy duty machinery that has a CAN-based vehicle network. People across the globe, rich or poor, use these vehicles. so there aren't exactly specific demographics we can point at. What we can look at in a defined matter, however, is what these various groups of communities will benefit from with this project; a well-curated module that will solve security risks involved with their everyday lives.

Area	Description	Examples
Public health, safety, and welfare	Creating a secure Mobile Vehicle Bus network will disallow malicious users across the grobe from creating threats in communities that are vulnerable to traffic incidents.	They won't be able to control the steering of the vehicle to hit pedestrians, harm the driver, or other vehicles on the road.
Global, cultural, and social	Every community and every culture deserves the right to feel safe, especially when it comes to mobile vehicle safety. Modern cars universally are pushing new and extensive safety measures, and this is one further step to ensure no bad actors can steal away that feeling of safety. The publicizing of this technology will also, in theory, boost car sales if the economy is doing well. A few of the older generations don't necessarily trust modern technology advancements.	By making a public statement that car companies and other vehicle manufacturer's are pushing for public safety, regulation and trust, more people will trust the technology and be more willing to use it. Some people drive older cars out of fear of fear for technology being abused and against their safety,
Environmental	However, the chips used in the Mobile Bus device will cause harm to the environment once the vehicle goes to a junkyard. (Very minorly as compared to everything else around it.)	Decomposition over time will pollute the environment that the vehicle's final resting place is in.
Economic	The economic impact that our project will have on the vehicle market, we can see impacting machinery in different ways. Companies will have to be careful how they let this adjust their profit margins. We can see companies being greedy with this technology, but that would also ruin their reputation on whether they're doing it for the money, or building a reputation in the community for a promising product.	While this is very important technology that can save lives, we don't believe it should cost thousands of dollars of an upcharge just for the general safety that a consumer, or the general public should have when it comes to mobile vehicles.

4.1.2 Prior Work/Solutions

We have a unique situation with our project in which our goal is to essentially peer review a solution which has been discovered. Our advisor, John Potter, has developed a potential solution to the J1939 security issue already, but due to limitations in his ability to have his work peer reviewed, he is unsure if there are shortcomings in his solution. The advantages we have in our project are thanks to John Potter's knowledge in this area. Rather than going into the project entirely blind, in a way we are able to follow in his footsteps while still remaining in the dark about his overall solution. This method will hopefully allow us to develop a different solution than his that's close enough that we are able to compare the two to find strengths and weaknesses in both.

In terms of solutions that allow the protection of J1939 CAN networks there are very few, and none like ours. The most common approach are devices that allow the monitoring of data on the CAN network, but these devices actually make the network MORE vulnerable (Arilou, NNG Group). The main benefit of our device is that it will go unnoticed and isn't intended to replace anything, but rather introduce the concept of cryptography into a CAN network. A direct pros and cons list of currently available solutions can be found below.

Our Solution	Arilou's Solution
PRO - Offers high vehicle safety	PRO - Offers moderate vehicle safety
PRO - Uses encryption to make CAN data secure	PRO - Allows users to read their CAN data
PRO - Installed by knowledgeable manufacturer	PRO - Tested and released to the market
CON - Makes CAN data more complex	CON - Requires users to learn and install on their own
CON - Currently not fully developed or tested	CON - Potentially opens up vehicle to vulnerabilities
	CON - Doesn't use encryption

Group, NNG. "How to Secure Commercial Vehicles: SAE J1939 Cybersecurity." *Arilou*, NNG Group, 3 May 2021, https://ariloutech.com/news/heavy-duty-vehicles-sae-j1939-cybersecurity/.

4.1.3 Technical Complexity

The design consists of multiple components because we will have to handle encrypting/decrypting messages sent in the CAN system. Part of this will be ways of verifying freshness of messages, if messages were tampered with, and the messages still getting where they need in sufficient time.

Currently in the industry there is no standard for encryption of messages in the CAN systemes, and many are vulnerable to attacks so this project looks to address that. Our client explained to us that there was a past project they did to come up with a solution to this, but that he's trying to see what we can come up with and if there's anything they didn't think of or consider that we will.

4.2 Design Exploration

4.2.1 Design Decisions

1. Choosing to use AES-128 for encryption because it fits the time constraints to encrypt/decrypt blocks of messages. This is important to the project success because our whole project has to do with how we are doing to secure messages on the CAN system, so the standard we use for encryption/decryption will be very important in how we do.

2. Using python - found lots of good resources and libraries for encryption/decryption. This is important to the project success because if we choose a language with good resources/libraries then it could have created unnecessary struggles for our group. Now we know we choose a language that won't hold us back.

3. laptop simulation - saves time so we don't have to test on the actual system and plug into the CAN network in the lab every time we want to test. We'll be able to test on our own laptops whenever we want. This is important to the project success because we would have wasted a lot more time testing than we had to.

4.2.2 Ideation

For picking python as the language we are using we considered a lot of different things. Using the lotus blossom technique we considered the following:

1. Python - language the group is second most familiar with, has a lot of resources/libraries for what we're doing
2. Rust - no one in the group is familiar with it, but we'd be interested in learning it, it's known for performance and memory safety
3. C - group is most familiar with due to past programming classes, it's a lower level language which means we would be responsible for a lot more memory management which could make the code more complicated
4. C++ - a potential alternative to C if we found that we needed the object oriented aspect of C++ over C's solely procedural oriented style.
5. A potentially unknown language - We were open to learning new things if the project required it, and we considered that there could be languages we hadn't heard of or worked with before that would end up being the best fit during the research phase.

4.2.3 Decision-Making and Trade-Off

	Pros	Cons
Python	Python is a simple language that has many libraries involving cybersecurity and encryption.	Python is a language that not all of us know in our group. So it would be a learning curve.
Rust	Rust is known for its memory safety and overall performance, recommended by our client.	None of us know this language, so it would be an even bigger learning curve than Python.
C	This language is the most familiar with everyone in our group as it is the most common language in the classes we have taken.	C is a lower level language that is not known for its memory management. This would make coding more complicated than we think it needs to be.
C++	Good alternative to C if we believe that Object-Orientation is needed for our project.	Not a familiar language to everyone, so a learning curve would ensue.
Unknown Language	The pros of an unknown language could be having a major benefit to encryption or other stuff that would fit our needs for this project.	An unknown language could cause a huge learning curve for our group, could have bad memory management, a low level language without any Object-Orientation, etc.

After the pros and cons, we decided on writing our project in C. This language is something we're all familiar with, so no one is left behind learning the syntax and potentially confused, while everyone else is writing the code. Debugging in a language you know can be difficult, just imagining trying to debug with a language we're not familiar with helped us solidify our choice of C.